RRB's Compliance with the Critical Infrastructure Assurance Program Report No. 00-13, August 9, 2000

This report represents the results of the Office of Inspector General's (OIG) review of the Railroad Retirement Board's (RRB) compliance with the critical infrastructure assurance program in the context of Presidential Decision Directive 63 (PDD-63).

BACKGROUND

The RRB is an independent agency in the executive branch of the Federal government. The RRB administers the health and welfare provisions of the Railroad Retirement Act by providing retirement benefits for eligible railroad employees, their spouses, widows and other survivors. During fiscal year 1999, the RRB paid approximately $8.25 billion in retirement and survivor benefits to about 748,000 beneficiaries. The RRB utilizes numerous mainframe and personal computer systems used for the computation and payment of these benefits.

In May 1998, the Clinton Administration issued a policy on Critical Infrastructure Protection: PDD-63, which called for a national effort to ensure the security of the nation's critical infrastructures. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. Critical infrastructures include, but are not limited to, telecommunications, banking and finance, energy, transportation, and essential government services.

The PDD-63 required that, by May 22, 2003, the United States should achieve and maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- The Federal government to perform essential national security missions and to ensure the general public health and safety;
- State and local governments to maintain order and to deliver minimum essential public services; and,
- The private sector to ensure orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

PDD-63 required every Federal department and agency to develop a plan for protecting its own critical infrastructure. These plans, required to be implemented by May 2000, should direct each agency to:

- Appoint a Chief Infrastructure Assurance Officer who has overall responsibility for protecting the agency's infrastructure;
- Identify cyber-based mission essential infrastructure and perform vulnerability assessments of this infrastructure;

- Establish an emergency management program;
- Establish a recovery and business resumption plan following a successful infrastructure attack; and,
- Establish effective critical infrastructure protection coordination with foreign, state and local governments, and industry.

PDD-63 called for a national plan coordination office to serve as the direct authority and official source of guidance for the Critical Infrastructure Assurance Program. The Clinton Administration established the Critical Infrastructure Assurance Office (CIAO) in May 1998.

PDD-63 also called for the national plan coordination office to produce a detailed plan to protect and defend America against cyber disruptions. The National Plan Version 1.0, issued January 2000, presented a comprehensive vision creating the necessary safeguards to protect the critical sectors of our economy, national security, public health, and safety.

On September 28, 1999, the President's Council on Integrity and Efficiency (PCIE) Audit Committee unanimously supported a proposal to initiate a review of the nation's critical infrastructure assurance program. The PCIE Audit Committee published a review guide for Federal OIGs on December 15, 1999. The National Aeronautics and Space Administration's OIG (NASA-OIG) is coordinating the PCIE review among Federal OIGs.

During March and April 2000, the National Security Agency conducted an information systems security assessment of the RRB. This assessment reviewed the RRB's security measures applied in safeguarding the agency's sensitive and essential information. The assessment identified major strengths in security, as well as areas of concern that could lead to potential security weaknesses.

OBJECTIVE, SCOPE AND METHODOLOGY

The overall objective of this review was to assess the adequacy of the RRB's critical infrastructure assurance program in the context of the May 1998 PDD-63. For this review, we used the December 1999 PCIE review guide. The scope encompassed the adequacy of the RRB's planning and assessment activities for protecting critical cyber-based infrastructures. We reviewed:

- RRB documents including computer security plans, Strategic Information Resource Management (IRM) Plan 1999-2004, and Administrative Circular IRM-7 (*Security Plans for Systems Containing Sensitive Information*);
- Prior RRB-OIG reports; and,
- Federal government documentation specific to critical infrastructure including *the National Plan for Information Systems Protection* – January 2000, *CIAO Practices for Securing Critical Information Assets* – January 2000, and GAO's October 1999 report entitled *Critical Infrastructure Protection, Comprehensive Strategy Can*

Draw on Year 2000 Experiences.

We held discussions with, and submitted monthly reports to, the NASA-OIG. In addition, we had discussions with the General Services Administration's (GSA) Critical Infrastructure Protection Plan Development Team, the Social Security Administration's OIG, and RRB management. We also attended an April 2000 PCIE mid-point conference for the critical infrastructure review in Washington, D.C.

We conducted the audit in accordance with generally accepted government auditing standards. Auditors performed the fieldwork at the RRB headquarters in Chicago, Illinois from January 2000 through June 2000.

Results of Review

The RRB has not fully complied with PDD-63 because the directive was not clear as to which agencies had to comply; there was a lack of communication from the CIAO; and GSA (lead agency for the Federal government sector) provided information to the RRB that was not consistent with the CIAO.

In addition, the RRB has not updated agency computer plans for eight of its nine computer systems since March 1995. A complete review and update for each system is required to be performed every two years as stated in Administrative Circular IRM-7, *Security Plans for Computer Systems Containing Sensitive Information*,

The details of our review are discussed below.

Compliance with PDD-63

The RRB has taken steps to begin addressing PDD-63. RRB management has designated a Critical Infrastructure Assurance Officer, who is the Chief Information Officer. The RRB has also submitted a request in the Fiscal Year 2002 budget to conduct a vulnerability assessment, and has started the process of enhancing existing directives and training material on security awareness.

However, the RRB has not completed a critical infrastructure assurance plan. The PDD-63 directed specific agencies to complete their initial critical infrastructure protection plans by November 1998. PDD-63 designated these agencies as lead agencies for sector liaison and lead agencies for special functions (see Appendix A). The RRB was not included on this PDD-63 list.

PDD-63 also directed the GSA, the Department of Commerce, and the Department of Defense to assist Federal agencies in the implementation of best practices for assurance within their individual agencies. GSA, as lead agency for the Federal government Critical Infrastructure Sector, held a briefing on October 13, 1998 that distinguished Primary, Secondary, and Special Function Agencies. Primary Agencies included agencies listed in

PDD-63. Secondary Agencies were additional agencies required to fully comply with the directive (see Appendix B). Special Function Agencies were agencies not specifically identified as Primary or Secondary Agencies. GSA instructed the Special Function Agencies to:

> *"…comply with existing guidance related to the protection of information systems, continuity of operations, and contingency planning contained in Office of Management and Budget (OMB) Circular A-130 Appendix III and other Executive Orders. It is suggested Agencies take on PDD-63 like planning efforts to ensure implementation."*

The RRB was not included in the list of Primary or Secondary Agencies. Therefore, the RRB was considered a Special Function Agency by default. As a result of the GSA briefing, the RRB followed GSA's guidance and did not establish critical infrastructure plans at the time.

In PDD-63, the President directed the development of the National Plan to prioritize critical infrastructure protection goals, principles and long-term planning efforts. This document (issued in January 2000) was the first attempt by any nation to develop a plan to defend its cyberspace. The National Plan addressed the responsibilities of Primary Agencies (termed Phase I Agencies in the National Plan) and Secondary Agencies (termed Phase II in the Plan), but does not address other agencies. The RRB was not listed in the Plan.

In April 2000, the NASA-OIG met with the CIAO to discuss issues and concerns regarding PDD-63 compliance. This meeting recognized the CIAO as the authoritative and official source for guidance on PDD-63. The CIAO noted that several key agencies were excluded from the listings of Primary and Secondary agencies (such as the U.S. Postal Office). However, the CIAO advised that all Federal agencies should comply with PDD-63 because the directive states that Federal government is to serve as a role model for private industry. The NASA-OIG has taken the position that agencies should have contacted the CIAO with questions on PDD-63 rather than relying on GSA's direction.

The CIAO has advised that Federal agencies should initially determine if they have critical assets as defined in PDD-63. The CIAO issued "Practices for Securing Critical Information Assets" in January 2000 to provide initial guidance for agencies in performing tasks necessary to comply with PDD-63. The first task is to use the *Infrastructure Asset Evaluation Survey* provided in this document to determine if agencies have critical assets. Once identified, agencies must secure those critical assets and related infrastructure components to fulfill their responsibilities of ensuring national security, national economic security, and public health and safety.

Recommendation:

The Bureau of Information Services should complete the *Infrastructure Asset Evaluation Survey* in the CIAO's "Practices for Securing Critical Information Assets" document to

determine if the RRB has critical assets (Recommendation 1).

Management's Response:

The Executive Committee agreed with our recommendation and has advised the Bureau of Information Services to implement corrective action.

Agency Computer Security Plans

During our review of agency computer security plans, we discovered that the RRB has not updated plans for eight of the agency's nine computer systems since March 1995. The RRB updated the plan for the ninth system in 1997. As stated in Administrative Circular IRM-7, *Security Plans for Computer Systems Containing Sensitive Information*, the RRB is required to perform a complete review and update for each system every two years.

The delay of updating the security plans jeopardizes the assurance that computer systems contain adequate measures to protect the confidentiality, integrity, and availability of sensitive information.

The Executive Board approved an update to Administrative Circular IRM-7 on May 22, 2000. The update contains guidance from the National Institute of Standards 800-18, which replaces and is significantly different from the current guidance (OMB Bulletin 90-08).

Recommendation:

The Bureau of Information Services should update computer security plans in accordance with Administrative Circular IRM-7 and National Institute of Standards 800-18 (Recommendation 2).

Management's Response:

The Executive Committee agreed with our recommendation and has advised the Bureau of Information Services to implement corrective action.

Appendix A

May 1998 Presidential Decision Directive 63
Listing of Specific Agencies Required to Comply

Lead Agencies for Sector Liaison

Department of Commerce
Department of Treasury
Environmental Protection Agency
Department of Transportation
Department of Justice/Federal Bureau of Investigations
Federal Emergency Management Agency
Department of Health and Human Services
Department of Energy

Lead Agencies for Special Functions

Department of Justice/Federal Bureau of Investigation
Central Intelligence Agency
Department of State and Foreign Affairs
Department of Defense

Appendix B

January 2000 National Plan
Agencies Required to Comply with PDD-63

Primary (Phase I) Agencies

All specific agencies previously listed in the May 1998 PDD-63
Department of Veterans Affairs
National Security Administration

Secondary (Phase II) Agencies

Department of Agriculture
Department of Education
Department of Housing and Urban Development
Department of Interior
Department of Labor
General Services Administration
National Aeronautics and Space Administration
Nuclear Regulatory Commission